

FIG. 2

USER GROUP MEMBERSHIP DATABASE 300

| i,    | 335 |      |      |      |   |      |
|-------|-----|------|------|------|---|------|
| ij    | 330 |      |      |      |   |      |
| Xi    | 325 |      |      |      |   |      |
| GROUP | 320 | 0001 | 0002 | 0003 | : | N000 |
|       |     | 301  | 302  | 303  | : | 305  |

| 'ALUES |   |   |   |   |   |
|--------|---|---|---|---|---|
| USER V | h | Ð | S | d | S |

FIG

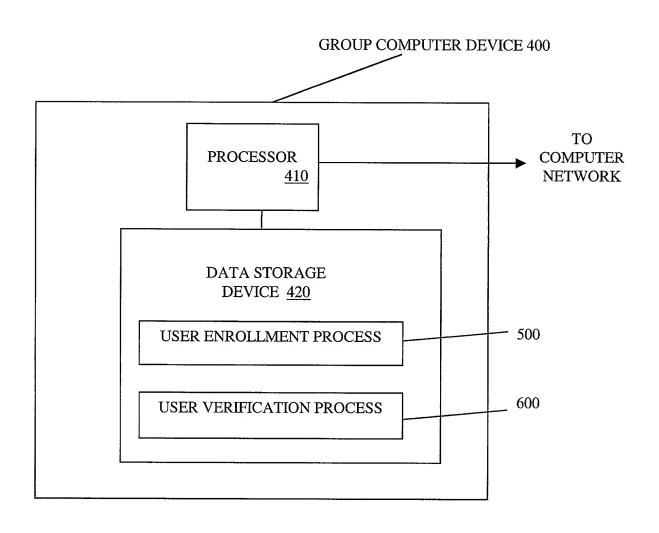


FIG. 4

User U Select  $x_i, h$  Compute  $ID_i = g^{x_ih}$ 

Group G Select  $k_i$  Compute  $G_i = g^{k_i h}$ 

Use Diffle-Hellman to exchange/setup the initial secret

Step 1: User U sends his  $ID_i$  to Group G

$$ID_i = g^{x_i h}$$

Step 2: Group G sends its ID  $G_i$  to User U

$$G_i = g^{k_i h}$$

Since  $ID_i^{k_i}=g^{x_ik_ih}=G_i^{x_i}$ , by now, both G and U have the shared secret  $g^{x_ik_ih}$ 

Step 3: Create the registration ID

U sends  $G_i^{x_i}x_i$  to G

G sends  $ID_i^{k_i}s_i$  to U

By now, both G and U have their registration handy, it is  $S_i = g^{s_i}$ 

FIG. 5

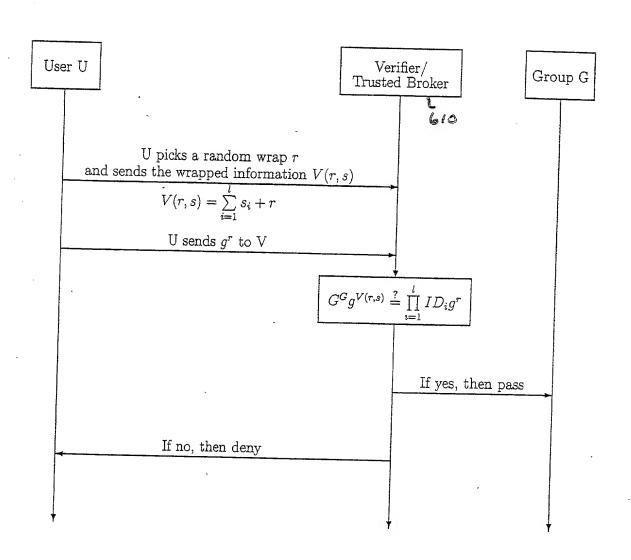


FIG. 6